Delaware Cyber Security Advisory Council (CSAC)

January 31, 2018 9:00 AM

Present Committee Members

James Collins	Department of Technology and Information (DTI)
Richard Gowen	Verizon
Mike Maksymow	Beebe Healthcare
Daniel Meadows	Delaware State Police
Lt. Col. Trevor Fulmer	National Guard
Renee Hupp	Delaware Emergency Management Agency

Also Present

Sandra Alexander	DTI
Aleine Cohen	DOJ
Erin Coombs	Jacobs
Daniel Eliot	University of Delaware
Lori Gorman	DTI
Megan Rosica	Jacobs
Eric Smith	JP Morgan Chase
Rob Walls	First Net
Greg Witte	G2, Inc.

I. Welcome and Introductions

a. The meeting commenced at 9:09 AM. J. Collins welcomed committee members and directed attendees to introduce themselves.

II. Review and Approval of Previous Meeting Minutes

a. The committee reviewed the minutes from the previous meeting held on September 27, 2017. Committee members had no revisions or comments. D. Meadows made the motion to accept the minutes and R. Hupp seconded. The motion was approved.

III. NIST Presentation

a. G. Witte presented information surrounding updates on the framework for improving critical infrastructure cybersecurity.

b. After a series of national workshops, a Cyber Security Framework (CSF) was developed as a guide for industry professionals to organize their practices and understand cybersecurity risks as well as strategies for mitigation. The goal of this flexible framework is for companies to encourage secure innovation and achieve their goals while keeping activities secure.

c. A comprehensive look at NIST's CSF can be found at the following link: https://www.nist.gov/cyberframework

d. Questions
    i. J. Collins asked if there would be events, meetings, or calls that the council could monitor regarding the NIST CSF.
        1. G. Witte responded that the website for the CSF allows those interested to sign up for updates as relevant news comes out. He also noted that the website includes an industry resource page which has tools developed for guidance.
    ii. J. Collins asked about tips for secure password management.
        1. G. Witte encouraged strong passwords that are longer and more memorable, such as phrases. He also suggested increased education to the public for more secure passwords and tips for keeping track of multiple passwords.
    iii. E. Starkey asked if this framework means moving away from ISO and more towards NIST.
        1. G. Witte responded that ISO is control based and NIST's CSF is not. The CSF allows for compliance with international standards. ISO maps well with CSF and more and more organizations are using both. CSF cannot be solely relied on.
    iv. R. Gowen wondered if there was any concept such as an underwriter's lab to help with some level of review to decrease vulnerability to attacks.
        1. G. Witte responded that this is a challenge and the real driver is the consumer. Risk is included in the framework and there must be an adequate level of protection depending on the location and use of technology or tool in question. The council can help to influence and drive conversation about risk and mitigation.
    v. A discussion occurred regarding security and vulnerability in different practices, e.g. medical technologies, emergency management, etc.

IV. Council Chair Updates

a. Legislation Updates/Council Membership
    i. Work is being done to alter the legislation in order to promote nonpublic language as to ensure that sensitive meeting conversations impacting critical infrastructure will not be shared publicly.
    ii. Membership
        1. E. Starkey explained that the League of Local Government seat is now vacant, as well as the Governor's Office appointee seat. The committee will wait to fill the seats and is open to suggestions for new members.

V. New Business

a. D. Elliot was formally commended and recognized by the committee. E. Starkey presented D. Elliot with a letter of commendation.

VI. Public Comment

a. D. Elliot has finalized the document to assist the small business community regarding Executive Order 180. He will be hiring a new person to replace his position.

VII. Old Business

a. Delaware Fusion Updates
    i. D. Meadows gave an overview of the Delaware Fusion Center and its goal to gather stakeholders to the Fusion Center as a conduit for information sharing. Stakeholders are currently waiting for Federal clearances to allow for open dialogue and produce tangible products on cyber mitigation and resiliency against cyber threats. D. Meadows discussed how the DIAC is proactively leveraging resources to expedite the procession of the clearance request.
    ii. M. Maksymow questioned the levels of clearances and if recipients of the information need clearances to review the products/reports generated by the DIAC.
        1. D. Meadows explained that as the process continues more individuals will be invited to participate. In the initial stages information will continue to be classified and then go through derivative declassification to allow for dissemination.
    iii. J. Collins asked if this concept could be expanded into other industries.
        1. D. Meadows responded that it will start in the financial sector and expand from there.

VIII. Executive Session

Executive Session pursuant to 29 Del. C. §§ 10002(l)(5), 10004(b)(6), & 10004(e)(2) to discuss sensitive portions of the Unclassified Department of Homeland Security Briefing

a. M. Maksymow made motion to go into executive session, E. Starkey seconded. Executive session began.

IX. Adjourn

a. J. Collins thanked attendees for participation in the meeting. R. Gowen made a motion to adjourn the meeting. M. Maksymow seconded. The meeting adjourned at 10:51 AM.